PATENT ABSTRACTS OF JAPAN

(11)Publication number : 01-180656
(43)Date of publication of application : 18.07.1989

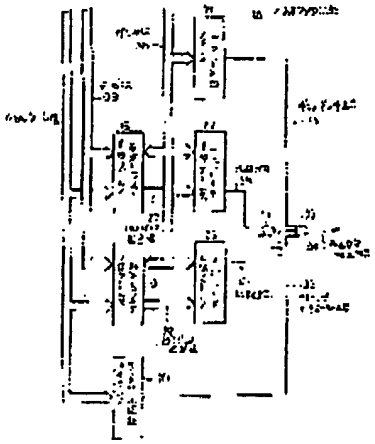
(51)Int.Cl. G06F 12/16

(21)Application number : 63-004599
(22)Date of filing : 12.01.1988

(71)Applicant : FUJI ELECTRIC CO LTD
(72)Inventor : KOMINE SHIGERU

(54) MEMORY PROTECTING DEVICE

(57)Abstract:
PURPOSE: To protect the memory area of another task by inhibiting a writing into the memory area except a writable area specified by a lower limit and an upper limit address setting registers, rewriting dynamically the values of both the registers by an OS at the time of switching the task and making only the area of the task being executed into the writable area.
CONSTITUTION: A lower limit address setting register 18 and an upper limit address setting registers 19 to set the writing inhibiting area are provided and the writing into the writing inhibiting area is detected by comparing addresses outputted from both the registers 18 and 19 and a CPU by a lower limit address comparator 22 and an upper address comparator 23. The contents of the lower limit and the upper limit address setting registers 18 and 19, that is, the writing inhibiting area is changed dynamically for every task by an operating system. Thus, a certain task is prevented from executing a wrong writing into the memory area or the i/O area of another task.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁(JP) ⑪特許出願公開

⑫公開特許公報(A) 平1-180656

⑤Int.Cl.⁴	識別記号	庁内整理番号	⑬公開 平成1年(1989)7月18日
G 06 F 12/16	310	H-7737-5B	

審査請求 未請求 請求項の数 1 (全6頁)

⑭発明の名称 メモリ保護装置

⑳特 願 昭63-4599
㉒出 願 昭63(1988)1月12日

㉑発明者 小 峯 繁 神奈川県川崎市川崎区田辺新田1番1号 富士電機株式会社内
㉑出願人 富士電機株式会社 神奈川県川崎市川崎区田辺新田1番1号
㉔代理人 弁理士 山口 巌

明 細 書

1. 発明の名称 メモリ保護装置

2. 特許請求の範囲

1) オペレーティング・システムによりマルチタスク処理を行い、かつ前記タスクはこのオペレーティング・システムを介してI/Oアクセスを行うように構成された電子計算機システムにおいて、

前記マルチタスク処理の開始時点、処理対象タスクの切換え時点、または処理中のタスクのI/Oアクセス時点において、前記オペレーティング・システムによって設定されるアドレス値であって、現に実行しようとするタスク、またはアクセスしようとするI/Oについてのアドレスの上限値および下限値(以下それぞれ上限アドレス設定値および下限アドレス設定値という)をそれぞれ設定される上限アドレス設定レジスタおよび下限アドレス設定レジスタと、

アドレスバス上に出力されるアドレス値が、前記上限アドレス設定レジスタおよび下限アドレス設定レジスタをそれぞれアクセスするアドレス値で無く、かつ前記上限アドレス設定値または下限アドレス設定値のいずれかを越えるものであり、さらにこのとき同時に制御バス上に書込信号が出力されていることを検出して異常警報信号を出力する不正書込検出手段と、を備えたことを特徴とするメモリ保護装置。

3. 発明の詳細な説明

【産業上の利用分野】

この発明は電子計算機のメモリ保護装置、特にメモリ管理機構を持たないマイクロプロセッサをCPUとし、マルチタスク処理(即ち複数タスクの並列処理)を行う電子計算機のメモリ保護装置に関する。

なお以下各図において同一の符号は同一もしくは相当部分を示す。また論理もしくはレベルHigh、Lowは単にH, Lと記すものとする。

【従来の技術】

メモリ管理機構を持たないマイクロプロセッサをCPUとして用いた電子計算機においては、プログラムの誤り(バグ)等によりCPUが暴走し

た場合，あるいはプログラムの誤りそのものにより、不正なアドレスに対してデータの書込みをしてしまうことがある。このような場合、プログラムが破壊されたりＩ／Ｏ機器が異常動作したりしてしまう。

このような不正な書込みに対してメモリを保護する方法として、メモリ空間を書込み可能な領域と書込み不可能な領域とに予め設定しておき、書込み不可能な領域に書込みが行われた場合に、ハードウェア的にこの不正な書込みを検出し、割込みによりＣＰＵに知らせるという方法がある。

例えば第３図のようなメモリマップを持つ電子計算機においてＲＡＭ領域１およびＩ／Ｏ領域３は書込み可能であり、未実装領域２およびＲＯＭ領域４は書込み禁止であると考える。

このような場合、書込み禁止領域への書込み動作を検出するために、第４図(a)のようにアドレスバスＡＢの上位側の一部の信号線６と，書込信号７とをアドレスデコード回路８によってデコードし、不正なアドレスに対する書込みに対して割込出力９に有効にし、図外のＣＰＵに割込みをかけるという方法が知られている。また第４図(b)のようにアドレスデコード回路８と同等の回路としてＲＯＭ10等を用いる方法もある。

【発明が解決しようとする問題点】

しかしながら、前記の方法は書込み可能領域としてのＩ／Ｏ領域３に対して何も保護がなされていないため、例えばプリンタ装置に異常なデータが出力されてしまうことを防ぐことができないという問題点がある。

また，マルチタスク処理を行うシステムにおいては、ＲＡＭ領域１に複数のプログラム（タスク）が同時に存在するが、従来の方法では各タスクのメモリ領域は全て書込み可能であるため、あるタスクが他のタスクのメモリ領域に対して不当な書込みを行うのを防ぐことができないという問題点が存在する。

そこで本発明の目的は、Ｉ／Ｏ領域への不正な書込みを防ぐことができ、しかもマルチタスク処理においてあるタスクの他のタスクのメモリ領域に対する不正な書込みを防ぐことができる手段を備えたメモリ保護装置を提供することにある。

【問題点を解決するための手段】

前記の目的を達成するために本発明の装置は『オペレーティング・システムによりマルチタスク処理を行い、かつ前記タスクはこのオペレーティング・システムを介してＩ／Ｏアクセスを行うように構成された電子計算機システムにおいて、

前記マルチタスク処理の開始時点，処理対象タスクの切換え時点，または処理中のタスクのｉ／Ｏアクセス時点において、前記オペレーティング・システムによって設定されるアドレス値であって、現に実行しようとするタスク，またはアクセスしようとするＩ／Ｏについてのアドレスの上限値および下限値（以下それぞれ上限アドレス設定値（28など）および下限アドレス設定値（27など）という）をそれぞれ設定される上限アドレス設定レジスタ（19など）および下限アドレス設定レジスタ（18など）と、

アドレスバス（ＡＢなど）上に出力されるアドレス値が、前記上限アドレス設定値レジスタおよび下限アドレス設定値レジスタをそれぞれアクセスするアドレス値で無く、かつ前記上限アドレス設定値または下限アドレス設定値のいずれかを越えるものであり、さらにこのとき同時に制御バス上に書込信号が出力されていることを検出して異常警報信号（不正書込検出出力91など）を出力する不正書込検出手段（アドレスデコード回路21，下限アドレスコンパレータ22，上限アドレスコンパレータ23，ＯＲゲート31，タイミングコントロール回路20，ＡＮＤゲート35など）と、を備えた』ものとする。

【作　用】

この発明は、書込み禁止領域を設定するための下限アドレス設定レジスタと上限アドレス設定レジスタとを設け、前記両レジスタとＣＰＵより出力されるアドレスとを下限アドレスコンパレータおよび上限アドレスコンパレータによって比較することにより書込み禁止領域への書込みを検出し、前記下限および上限アドレス設定レジスタの内容，

すなわち書込み禁止領域を、ＯＳ（オペレーティング・システム）によってタスクごとに動的に変更することによって、あるタスクが他のタスクのメモリ領域やＩ／Ｏ領域に対して不正な書込みを行うのを防ぐようにしたものである。

【実施例】

第２図は本発明による電子計算機の構成を示す。同図においてＣＰＵ部11はマイクロプロセッサおよびクロックジェネレータ，バスコントローラ，バスバッファ等の周辺回路からなり、この部分11はメモリ管理機構を持っていない。ＣＰＵ部11よりアドレスバスＡＢ，データバスＤＢ，制御バスＣＢからなる主バスＭＢを介して、メモリ部12，Ｉ／Ｏ部13，不正書込検出部14が接続されている。メモリ部12はＲＡＭ，ＲＯＭ，制御回路等から成り、Ｉ／Ｏ部13はＩ／Ｏ制御回路等から成る。Ｉ／Ｏ部13はＩ／Ｏバス17を介してＩ／Ｏ装置15と接続されている。

次に不正書込検出部14の構成を第１図に示す。マルチタクス処理を行う電子計算機システムにおいては、ＯＳ（オペレーティング・システム）がタスク管理やＩ／Ｏ管理等を全て行う。アプリケーション・プログラム，従ってタスクからはＩ／Ｏ装置との直接のやりとりは行わず、ＯＳにＩ／Ｏ装置15とのやりとりを依頼する。

マルチタスク用ＯＳは各タスクの実行状況を記憶しておく領域を持っている。この記憶領域は通常ＴＣＢ（Ｔａｓｋ　Ｃｏｎｔｒｏｌ　Ｂｌｏｃｋ）と呼ばれ、各々のタスクが実行中断された場合のレジスタ値などが格納されている。

本発明においては各タスクごとに、そのタスクのメモリ領域の下限(最低位)アドレスと上限（最高位）アドレスとを考える。各タスクごとの下限アドレス，上限アドレスが実際に決定するのは、ＯＳが補助記憶装置（ハードディスク，フロッピーディスク等）からプログラム（ロードモジュール）をロードするときであるが、この際にＯＳは各タスクごとのＴＣＢの中に、そのタスクのメモリ領域の下限アドレスと上限アドレスとを格納するものとする。

ＯＳは各タスク切換え時に、現在実行中のタスク（タスク１とする）のレジスタ値をタスク１のＴＣＢ（ＴＣＢ１）に格納し、これから実行しようとするタスク（タスク２）のレジスタ値をタスク２のＴＣＢ（ＴＣＢ２）よりロードする。さらにＴＣＢ２中のタスク２の下限アドレスを下限アドレス設定レジスタ18に設定し、タスク２の上限アドレスを上限アドレス設定レジスタ19に設定する。このようにして下限アドレス設定レジスタ18，上限アドレス設定レジスタ19には、それぞれ現在実行中のタスクの下限アドレス，上限アドレスが設定されることになる。

そしてＣＰＵが現在、アドレスバスＡＢに出力しているアドレスと、下限アドレス設定レジスタ18への設定値27とを下限アドレスコンパレータ22により、また同じく前記アドレスと上限アドレス設定レジスタ19への設定値28とを上限アドレスコンパレータ23により、それぞれ比較する。

従ってもしＣＰＵが現在実行中のタスクのアドレス領域より低位のアドレスにアクセスした場合，すなわち下限アドレス設定値27よりアドレスバスＡＢに出力されているアドレス値が小さい場合には下限アドレスコンパレータ22の比較出力29はＨレベルになり、この比較出力29を入力信号とするＯＲゲート31の出力32もＨレベルになる。同様にＣＰＵが現在実行中のタスクのアドレス領域より高位のアドレスにアクセスした場合，すなわち上限アドレス設定値28よりアドレスバスＡＢに出力されているアドレス値が大きい場合にも上限アドレスコンパレータ23の比較出力30はＨレベルになり、この比較出力30をも入力信号とする前記ＯＲゲート31の出力もＨレベルになる。

つまりＯＲゲート31の出力32は、上限および下限アドレス設定レジスタ18，19により定められる，現在実行中のタスクのメモリ領域以外のアドレスをＣＰＵがアドレスバスＡＢに出力した場合にＨレベルになる。

しかしＣＰＵは常に有効なアドレスをアドレスバスＡＢに出力しているわけではなく、あるアドレスから別のアドレスに切換わる場合や，バスア

クセスを行わない場合などにアドレスバスＡＢに出力されるアドレスは不定となる。

またタスク切換えは割込みによりタスクからＯＳに制御が移ることによりＯＳによって行われる。従ってこのとき割込みベクタ領域やＯＳの命令コード領域のアドレスがアドレスバスＡＢ上に出力されるが、このこのアドレスは不当なアドレスとしなければならない。つまり、あるタスクの領域以外書込みは禁止するが、読出しは自由に行えるものとする。読出しによりメモリ内容が破壊されることはないので、メモリ保護のためには書込みのみ禁止すればよい。

そこでタイミングコントロール回路20は、ＣＰＵが書込み動作を行う場合で、しかもアドレスが確実に有効であるタイミングでのみその出力信号（タイミングコントロール信号）33がＨレベルになるようにする。これによってアドレスが不定の期間や、読出し動作の場合に誤った割込信号としての不定書込検出出力9AがＡＮＤゲート35からＣＰＵに入るのを防ぐ。

先に述べたようにマルチタスクシステムではＩ／ＯアクセスはＯＳを通して行われる。特に本方式においてはアプリケーションプログラムがＩ／Ｏ領域に直接書込みを行うことは不可能であるようにする。なぜならＩ／Ｏのアドレスはタスクのアドレス領域の外側にあり、タスクのアドレス領域のみが書込み可能な領域であるからである。アプリケーションプログラムはＩ／Ｏアクセスを行う場合、割込みまたはＣＡＬＬ命令によってＯＳに制御を移す。このとき割込みベクタやＯＳの命令コード領域は書込み禁止ではあるが、読出しは可能であるのでＯＳに制御を移しＯＳの命令コードをＣＰＵが実行することが可能である。ＯＳは上限および下限アドレス設定レジスタ18，19に値を設定し直し、Ｉ／Ｏアドレス領域に書込むことが可能なようにしてからＩ／Ｏアドレスへのアクセスを行う。

ところが上限および下限アドレス設定レジスタ18，19をアクセスするためのアドレス値もＩ／Ｏアドレスに割付けられているので、このままでは両レジスタに書込みを行うことができない。従って下限および上限アドレス設定レジスタ18，19へは両レジスタのアドレス値にかかわらず，すなわち現在の書込み可能領域にかかわらず、常に書込み可能でなければならない。そこで常にこの両レジスタ18，19への書込みを可能とするのがアドレスデコード回路21で、その出力信号（アドレスデコード信号）34はアドレスバスＡＢの値が下限または上限アドレス設定レジスタ18，19をアクセスするアドレス値である場合のみＬレベルとなり、それ以外の場合はＨレベルとなる。これにより下限または上限アドレス設定レジスタ18，19へのアドレス設定値27または28の書込みの際は、不正書込検出部14の検出出力、つまりＡＮＤゲート35からの不正書込検出出力9Aが有効にならず、両レジスタ18，19へは常に書込み可能となる。

以上よりＣＰＵがアドレスバスＡＢに出力するアドレスが、下限および上限アドレス設定レジスタ18，19により規定される書込み可能な領域にあるか、または下限，上限アドレス設定レジスタ18，19への書込みのための（つまり該レジスタ18，19をアクセスする）アドレスであるかでなければ、不正書込検出出力9AはＨレベルとなる。この出力9AをＣＰＵ割込信号として入力することにより、ＣＰＵは不正な書込みを検知できる。

なお、下限，上限アドレス設定レジスタ18，19へは常に書込み可能であるが、不正な書込みにより偶然これらのレジスタに何らかの値を書込み、しかも次のどこかのアドレスに対する書込みで割込みが起らないという確率は非常に低い。

ＯＳは不正書込検出出力9AがＨレベルとなり，割込みとしてＣＰＵに入力されることによりエラー処理ルーチンに入り、エラーメッセージの出力，異常動作したタスクの実行停止，場合によってはシステム全体の停止等の処理を行う。

【発明の効果】

この発明によれば、下限および上限アドレス設定レジスタによって定まる書込み可能領域以外のメモリ領域は書込み禁止とし、ＯＳにより前記両レジスタの値をタスク切換え時に動的に書換え、

実行中のタスクの領域のみを書込み可能領域としたので他のタスクのメモリ領域の保護を行うことができる。

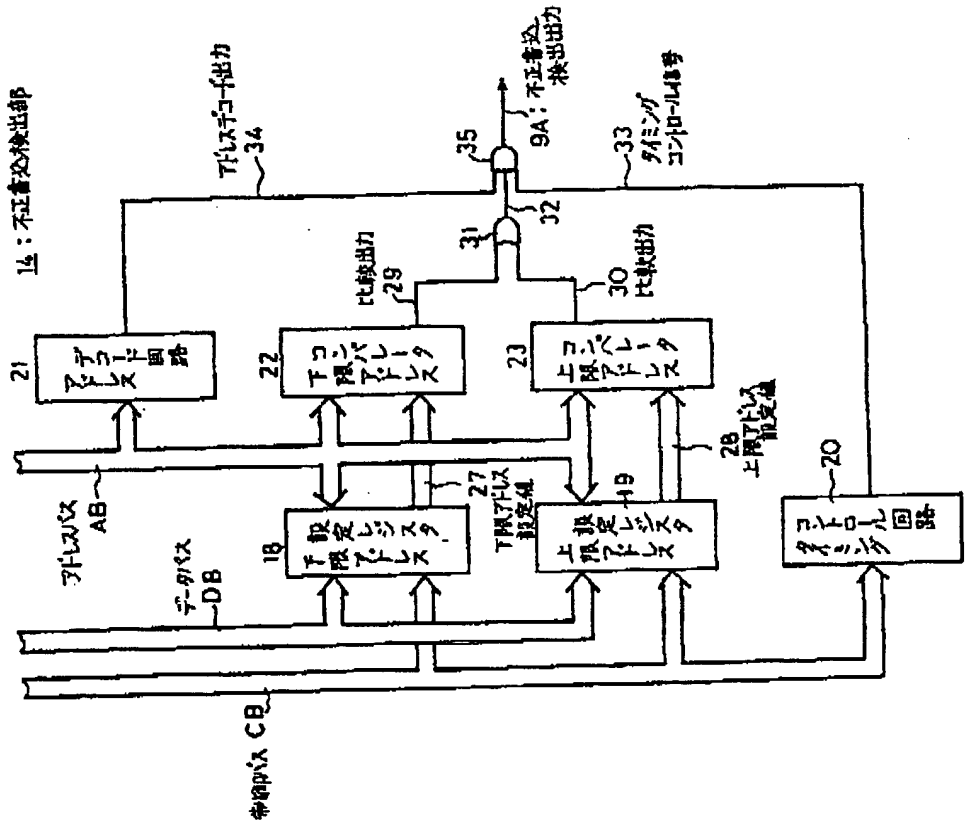
また、i／O領域への書込みはOSのみが行うことができるようにしたので、i／O機器の異常動作を防ぐことができる。

4．図面の簡単な説明

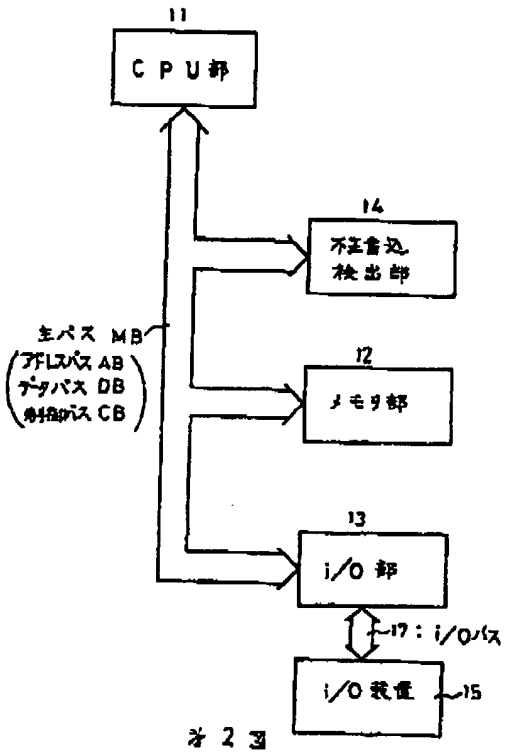
第1図は本発明の一実施例としての不正書込検出部の構成を示すブロック図、第2図は同じく電子計算機システムの要部構成を示すブロック図、第3図は電子計算機システムのメモリマップ例を示す図、第4図は従来のメモリ保護方式の要部構成を示すブロック図である。

11—CPU部、14—不正書込検出部、18—下限アドレス設定レジスタ、19—上限アドレス設定レジスタ、20—タイミングコントロール回路、21—アドレスデコード回路、22—下限アドレスコンパレータ、23—上限アドレスコンパレータ、31—ORゲート、35—ANDゲート、AB—アドレスバス、DB—データバス、CB—制御バス、9A—不正書込検出出力。

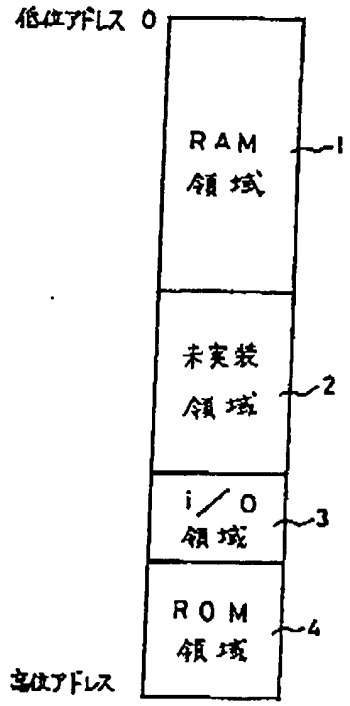
代理人弁理士 山口 巖



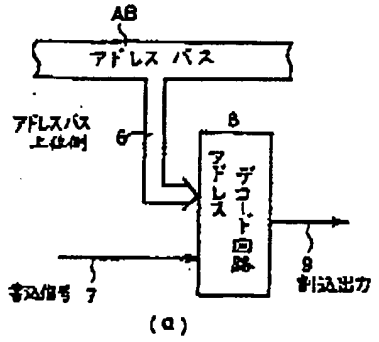
第1図



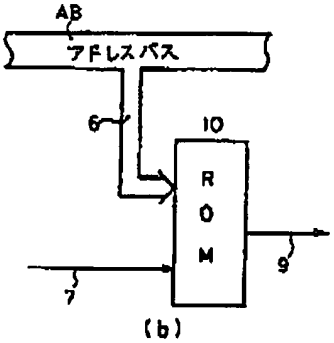
第2図



第3図



(a)



(b)

第4図